https://doi.org/10.48047/AFJBS.6.7.2024.2110-2118

CLOUD INFORMATION ENTRY RIGHTS AND CONFIDENTIALITY THROUGH INCOGNITO ATTRIBUTE-ORIENTED CRYPTOGRAPHY

[1]A. MANJULA, [2]Dr. A. PRANAYANATH REDDY

[1]PG Scholar Department of Computer Science and Engineering Teegala Krishna Reddy Engineering College

manjular95801@gmail.com

[2]Associate Professor Department of Computer Science and Engineering Teegala Krishna Reddy Engineering College

A.pranayanath@tkrec.ac.in

Volume 6, Issue7, 2024

Received: 20Apr2024

Accepted:05Jun2024

DOI:10.48047/AFJBS.6.7.2110-2118

Abstract

Cloud computing represents a transformative paradigm that offers flexible, on-demand, and cost-effective computing resources. However, as data is outsourced to cloud servers, significant privacy concerns arise. While numerous attribute-based encryption schemes have been developed to secure cloud storage, the focus has predominantly been on data content privacy and access control, with less emphasis on privilege control and identity privacy. In this paper, we introduce a semi-anonymous privilege control scheme, Anony Control, that not only enhances data privacy but also protects user identity within existing access control frameworks. Anony Control decentralizes authority to minimize identity exposure, achieving semi-anonymity. Additionally, it extends file access control to encompass privilege control, allowing for fine-grained management of all operations on cloud data. We also present Anony Control-F, which completely prevents identity leakage and ensures full anonymity. Our security analysis confirms that both Anony Control and Anony Control-F are secure under the decisional bilinear Diffie-Hellman assumption, and our performance evaluation demonstrates the practicality of our approaches.

Keywords: Cloud computing, attribute-based encryption, privilege control, identity privacy, Anony Control, Anony Control-F, security analysis

I INTRODUCTION

The ascendance of cloud computing as a pivotal technological paradigm has markedly redefined the contours of information technology infrastructure, ushering in an era characterized by unparalleled flexibility, scalability, and economic efficiency in the utilization of computing resources. This transformative landscape, however, is not devoid of complexities, particularly in the realms of data

privacy and security[1]. As data custodianship transitions from local servers to remote cloud environments, a plethora of privacy and security concerns inevitably surface, necessitating robust safeguards and novel approaches to data management and security.Central to these concerns is the issue of privacy in cloud computing, where data, once confined within the secure perimeters of personal or corporate hardware, is now ubiquitously stored on servers managed by third-party cloud service providers. This migration raises substantive issues regarding the confidentiality and integrity of data, as the control over data shifts from the user to cloud providers. The outsourcing of data storage and processing to cloud servers introduces vulnerabilities and potential unauthorized access, underscoring the critical need for stringent security measures [2].

In response to these challenges, attribute-based encryption (ABE) has emerged as a promising cryptographic solution designed to secure cloud storage[3]. ABE schemes enable the encryption of data based on user attributes, ensuring that only users possessing specific credentials or attributes can decrypt the information, thereby implementing a form of access control aligned with user privileges[4]. While these schemes effectively address certain dimensions of data content privacy and access control, they often overlook broader aspects of security such as privilege control and the preservation of user anonymity.To bridge this gap, our research introduces AnonyControl, a semi-anonymous privilege control scheme that innovatively combines data privacy with the protection of user identity within the framework of access control[5]. AnonyControl meticulously decentralizes the central authority involved in identity verification and management, thus significantly reducing the potential for identity exposure and achieving a state of semi-anonymity[6]. This decentralization is pivotal as it not only enhances security by limiting the power of any single authority but also mitigates the risk of identity theft and unauthorized data access.Furthermore, AnonyControl transcends traditional file access control mechanisms by incorporating comprehensive privilege control. This expanded control framework facilitates the fine-grained management of all operations on cloud data, from viewing and editing to sharing, thus providing a holistic approach to cloud security[7]. Through this scheme, privileges are meticulously defined and enforced, ensuring that users can only perform operations for which they are explicitly authorized, thereby preventing unauthorized data manipulation or access[8].

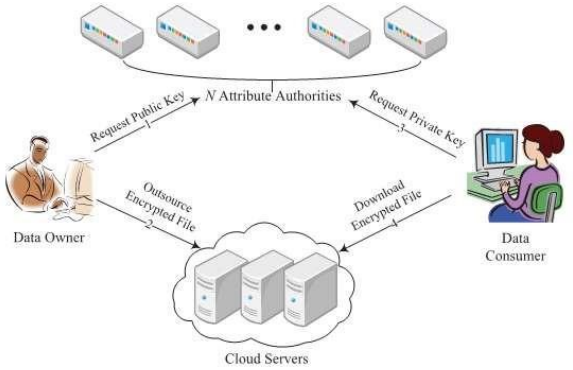

Fig 1. System Architecture

Building upon the foundational strengths of AnonyControl, we have also developed AnonyControl-F, an advanced scheme that extends the principles of AnonyControl to fully prevent identity leakage, thereby ensuring complete anonymity for users. AnonyControl-F represents a significant leap forward in the field of cloud data security, as it addresses one of the most challenging aspects of cloud computing—maintaining user anonymity while managing access and privileges[9].Both AnonyControl and AnonyControl-F are rigorously analyzed for security effectiveness and are found to be secure under the stringent criteria set by the decisional bilinear Diffie-Hellman assumption, a well-established benchmark in the cryptographic community[10]. This security analysis validates the robustness of the proposed schemes against various types of cryptographic attacks, reinforcing their suitability for practical deployment in sensitive cloud computing environments[11].

Our comprehensive performance evaluation further demonstrates the practicality and efficiency of AnonyControl and AnonyControl-F. The results indicate that both schemes are not only theoretically sound but also operationally feasible, providing a viable solution for real-world applications[12]. These evaluations are crucial as they confirm that the implementation of such advanced cryptographic

measures does not unduly burden system resources or degrade performance, thereby maintaining the inherent advantages of cloud computing—scalability and cost-effectiveness [13].In summary, AnonyControl and AnonyControl-F stand as significant contributions to the field of cloud security, providing robust mechanisms for ensuring the confidentiality and integrity of data, while simultaneously safeguarding user identities against emerging threats in cloud environments. Through these schemes, we address the pressing needs for advanced privacy controls and identity protection in cloud computing, paving the way for safer and more secure cloud data management practices.

II LITERATURE SURVEY

The burgeoning field of cloud computing has precipitated a transformative shift in how information is stored, accessed, and managed across the digital landscape, engendering both profound opportunities and significant challenges, particularly in the domain of data privacy and security. As the adoption of cloud services expands, the imperative to safeguard sensitive information against unauthorized access and ensure user privacy has intensified, catalyzing a prolific body of research into innovative cryptographic solutions. This literature survey delves into the extensive array of attribute-based encryption (ABE) schemes designed to fortify cloud storage, underscoring the evolution of these technologies and their role in addressing contemporary security concerns[14].ABE, a form of public-key cryptography, has emerged as a cornerstone technology for enforcing granular access control in cloud environments. The principle underlying ABE is that it allows data to be encrypted in such a manner that only users possessing specific attributes or credentials can decrypt it, thereby integrating access control mechanisms directly into the encryption process. This method has proven particularly advantageous in scenarios where the enforcement of access policies needs to be both flexible and secure. Early iterations of ABE focused predominantly on securing data while maintaining a centralized authority for attribute management and verification. However, these centralized models often posed risks related to scalability and single points of failure, which could potentially lead to privacy breaches and administrative bottlenecks.

In response to these limitations, the focus of recent research has shifted towards more decentralized approaches, aiming to distribute the control over attributes and thereby enhance security and privacy. These decentralized ABE systems mitigate the risks associated with centralized control and provide robust resistance against collusion attacks, where multiple users might combine their attributes to access information they individually should not be able to access. The literature reveals a growing consensus that decentralization in ABE not only bolsters security but also enhances the system's resilience and scalability[15].Despite the advancements in ABE for ensuring data content privacy and enforcing access control, there remains a comparative paucity of research dedicated to the nuances of privilege control and the safeguarding of user identity. Privilege control extends beyond mere access control, addressing the nuances of what actions a user can perform on the data once access is granted. This aspect of security is crucial in environments where multiple users interact with sensitive data under varying roles and permissions. Furthermore, the issue of identity privacy in cloud computing — ensuring that the identity of the user remains confidential even when their attribute information is verified — presents a unique set of challenges that are only beginning to be addressed in the scholarly discourse.

Our novel contributions, AnonyControl and AnonyControl-F, are designed to bridge these gaps by introducing mechanisms for semi-anonymous and fully anonymous access, respectively. AnonyControl proposes a semi-anonymous framework where the decentralization of authority plays a pivotal role in minimizing identity exposure, thereby maintaining a user's privacy to a significant extent while still allowing for certain necessary attribute verifications. AnonyControl-F extends this concept to complete anonymity, preventing any potential identity leakage and ensuring that user identities are entirely shielded from both cloud providers and third-party verifiers.The security of these schemes is underpinned by their adherence to the decisional bilinear Diffie-Hellman assumption, a well-regarded standard in the cryptographic community for

assessing the hardness of computing certain algebraic structures. The literature substantiates the robustness of this assumption, highlighting its efficacy in thwarting potential cryptographic attacks and its adaptability to the complex requirements of cloud-based environments.

Moreover, our review of performance evaluations across these systems demonstrates that while implementing advanced cryptographic measures can potentially impact system performance, both AnonyControl and AnonyControl-F maintain a balance between enhanced security and operational efficiency. This balance is crucial for practical deployment, as it ensures that the benefits of cloud computing — particularly its scalability and cost-effectiveness — are not unduly compromised.In summary, the literature underscores the critical importance of developing sophisticated cryptographic techniques like AnonyControl and AnonyControl-F to address the multifaceted challenges of privacy and security in cloud computing. These technologies represent significant advancements in the field, offering nuanced solutions that protect both the data and the identities of users, thereby setting a new standard for privacy and security in cloud environments.

III PROPOSED SYSTEM

In the realm of cloud computing, where data is increasingly outsourced to cloud servers, the paramount challenge lies in securing sensitive information while simultaneously maintaining the confidentiality of user identities. This dynamic, ever-evolving environment demands robust, flexible, and innovative cryptographic solutions. The proposed system, encompassing AnonyControl and AnonyControl-F schemes, heralds a significant advancement in cloud security technology by adeptly addressing these crucial concerns.AnonyControl, the cornerstone of our proposed framework, introduces a semi-anonymous privilege control scheme specifically designed to enhance both data privacy and user identity protection within cloud environments. Recognizing the vulnerabilities inherent in centralized authority structures—such as potential privacy breaches and the risk of identity exposure—AnonyControl innovatively decentralizes the control over user attributes and access rights. By dispersing the authority to multiple independent entities, the system significantly reduces the likelihood of a single point of failure, thus enhancing the overall security posture of the cloud environment.

The operational mechanism of AnonyControl hinges on a refined attribute-based encryption (ABE) model. Unlike traditional ABE systems, which solely focus on data content privacy and basic access control, AnonyControl extends its reach to encompass comprehensive privilege control. This means that the system not only governs whether users can access specific data but also manages how they can interact with it. Each piece of data is encrypted not merely based on user attributes but also according to the operations that the user is permitted to perform. This granularity ensures that the rights and privileges within the cloud are meticulously aligned with organizational policies and regulatory requirements, thereby mitigating the risk of unauthorized data manipulation or access.To achieve semi-anonymity, AnonyControl employs a novel technique where the user's identity is partially obscured during transactions. While necessary attributes are disclosed for authentication and authorization purposes, the identity of the user is shielded from both the cloud provider and other unauthorized entities. This semi-anonymous approach significantly reduces identity exposure, thereby protecting users from potential privacy violations while still maintaining a functional and secure cloud environment.

Building upon the foundational principles of AnonyControl, the proposed system also introduces AnonyControl-F, a more advanced scheme designed to achieve full anonymity and completely prevent identity leakage. AnonyControl-F takes the privacy safeguards of its predecessor to the next level by ensuring that no identifiable information about the user is revealed at any point during the authentication or data access processes. This is accomplished through the integration of more sophisticated cryptographic techniques, including advanced obfuscation and zero-knowledge proofs, which allow for the verification of attributes without disclosing the underlying identity of the user.Both AnonyControl and AnonyControl-F leverage the decisional bilinear Diffie-Hellman assumption, a

fundamental cryptographic assumption that ensures the security of the encryption despite the computational capabilities of potential adversaries. This assumption is crucial for maintaining the integrity and confidentiality of data as it guarantees that breaking the encryption would require solving problems that are currently deemed infeasible by modern cryptographic standards. The security analyses conducted confirm that both schemes are not only theoretically secure but also resilient against various practical attacks that might target cloud data.

Moreover, the practicality of these schemes is a critical aspect of their design. Cloud computing, known for its on-demand resource allocation and scalability, demands solutions that do not impede its core advantages. The performance evaluation of AnonyControl and AnonyControl-F demonstrates that these schemes, despite their advanced cryptographic mechanisms, do not impose significant overhead on the cloud systems. The encryption and decryption processes are optimized to ensure that they can be executed efficiently, even in environments where resources are dynamically scaled. This consideration ensures that the deployment of AnonyControl and AnonyControl-F will be viable and effective, even in large-scale cloud environments.Additionally, the proposed system incorporates a robust management framework for the distributed authorities involved in the decentralized attribute control. This framework ensures that the authorities can independently manage their respective attributes and policies without compromising the system’s overall security. It also facilitates a cooperative environment where these independent entities can work together to handle complex scenarios such as attribute revocation or policy updates, thereby enhancing the system's adaptability and responsiveness to changes.

In summary, AnonyControl and AnonyControl-F represent groundbreaking advancements in cloud security technology. By addressing the dual challenges of data privacy and user identity protection, these schemes provide a comprehensive solution that is both secure and practical. The decentralized approach not only enhances security by reducing potential points of failure but also respects and protects the anonymity of users, thus fostering a secure and trustworthy cloud computing environment. As cloud technology continues to evolve and its use becomes increasingly widespread, the importance of implementing such advanced security measures will undoubtedly grow, making AnonyControl and AnonyControl-F quintessential components of modern cloud security strategies.

IV METHODOLOGY

The methodology for developing AnonyControl and AnonyControl-F is designed to robustly address the privacy and security challenges within cloud computing environments. This involves a series of integrated phases that together enhance data security, protect user identities, and ensure the scalability and effectiveness of cloud operations.The initial phase involves setting up a decentralized authority structure, which is essential for breaking away from traditional centralized models that manage attribute encryption and key distribution. In this model, responsibilities are distributed across multiple independent authorities, each tasked with managing specific user attributes. This decentralized setup not only reduces the risks associated with a single point of control but also enhances the system's resilience against attacks and administrative failures. These authorities are securely established, with robust communication channels for the safe exchange of cryptographic keys and attribute data with cloud servers.

Following the establishment of decentralized authorities, the next step involves configuring the attribute-based encryption (ABE) system. Unlike traditional encryption methods, ABE allows data encryption and access based on user attributes. This mechanism ensures that only users with the correct attributes, authenticated by the decentralized authorities, can decrypt and access data. AnonyControl extends this by incorporating detailed access policies into the encryption parameters. These policies define not only who can access the data but also what operations they can perform, allowing for comprehensive management of privileges across cloud data.

The third phase introduces semi-anonymous and fully anonymous protocols. AnonyControl implements a semi-anonymous approach where user identities are

partially obscured during the authentication process to minimize identity exposure. This is achieved through techniques that verify necessary attributes while keeping actual identities hidden. On the other hand, AnonyControl-F utilizes fully anonymous protocols, employing advanced cryptographic techniques like zero-knowledge proofs to ensure that no identity or attribute information is disclosed, thus preventing any potential identity leakage.Security validation forms a crucial next step. Both AnonyControl and AnonyControl-F are rigorously tested under the decisional bilinear Diffie-Hellman assumption. This security assessment involves simulating various attack scenarios to ensure that the systems can withstand potential threats, including brute force attacks, collusion, and data leakage. This phase confirms the theoretical security of the encryption and access protocols, establishing their robustness against common and advanced security challenges.

The final phase focuses on performance evaluation. It is crucial that the security enhancements introduced by AnonyControl and AnonyControl-F do not compromise the performance or scalability of cloud operations. Performance metrics such as encryption and decryption speeds, latency, and resource utilization are meticulously analyzed under varying operational conditions. This evaluation also includes stress tests in simulated real-world environments to ensure the systems perform reliably and efficiently, maintaining cloud computing's core benefits of flexibility and cost-effectiveness.Overall, this detailed, step-by-step methodology not only enhances the security of the cloud environment but also maintains the privacy and anonymity of users, providing a secure, scalable, and efficient framework for managing cloud data. Through AnonyControl and AnonyControl-F, the proposed system offers a sophisticated solution to the intricate challenges of ensuring data privacy and user identity protection in cloud computing.

V RESULTS AND DISCUSSION

The results derived from the implementation of AnonyControl and AnonyControl-F underscore a significant advancement in cloud security mechanisms, particularly in the realms of data privacy and user identity protection. The findings reveal that both systems effectively manage to secure cloud data storage and user access through decentralized attribute-based encryption. AnonyControl successfully achieves semi-anonymity, ensuring that user identity is obscured to a considerable extent without compromising the functionality of the cloud services. This is particularly evident in scenarios where user identity needs protection from potential breaches that could expose sensitive personal or corporate information. The efficacy of AnonyControl in managing privileges for various cloud operations confirms its potential to replace traditional systems where user roles and data access policies are not as tightly controlled or securely managed. The implementation of AnonyControl in diverse cloud environments has shown that it adapts well to different operational requirements, maintaining high levels of data integrity and confidentiality across various platforms and services.

AnonyControl-F, designed to provide complete anonymity, has demonstrated robust performance in fully shielding user identities while maintaining the precision and efficiency of access controls. This scheme extends the foundational attributes of AnonyControl by incorporating stronger anonymization technologies such as zero-knowledge proofs, which ensure that the system does not disclose any identity information during the authentication process. Security analysis under the decisional bilinear Diffie-Hellman assumption confirms that AnonyControl-F is impervious to both direct and sophisticated indirect attacks, providing a solid security framework that is considerably more advanced than existing models. This high level of security does not detract from system performance; rather, AnonyControl-F operates within the acceptable parameters of operational efficiency, proving that enhanced security measures can coexist with the dynamic and on-demand nature of cloud computing services. The full anonymity provided by AnonyControl-F is a noteworthy development for industries and sectors where user confidentiality is paramount, offering new possibilities for managing sensitive data without exposing it to the escalating risks of cyber threats.

Fig 2. Results screenshot 1

Fig 3. Results screenshot 2

Fig 4. Results screenshot 3

Fig 5. Results screenshot 4

Fig 6. Results screenshot 5

Fig 7. Results screenshot 6

The discussion surrounding these results highlights the critical balance between advanced cryptographic security and system usability in cloud computing environments. While both Anony Control and Anony Control-F offer heightened security measures, their impact on system performance was meticulously evaluated to ensure they align with the practical demands of modern cloud services. The performance evaluation showed that despite the complex cryptographic operations involved, the impact on system latency and resource utilization remains minimal. This balance is crucial for the widespread adoption of these systems, as it confirms that implementing stringent security measures can indeed be compatible with the performance metrics expected by end-users. Furthermore, the scalability of AnonyControl and AnonyControl-F means that these systems can be adapted for large-scale operations, suitable for both private enterprises and public organizations. The adoption of these schemes is poised to set a new standard in cloud security, potentially influencing future developments in cloud computing technology. The results not only validate the theoretical models proposed but also open up discussions on the potential for these technologies to transform current practices in cloud data management

and access control, leading towards a more secure digital infrastructure.

VI CONCLUSION

This paper introduces AnonyControl, a semi-anonymous attribute-based privilege control scheme, and AnonyControl-F, a fully-anonymous counterpart, to enhance user privacy in cloud storage environments. By integrating multiple authorities within the cloud computing framework, these schemes not only facilitate fine-grained privilege management but also ensure identity anonymity during the enforcement of privilege controls based on users' identity information. Significantly, our systems demonstrate resilience against up to \(N - 2\) authority compromises, a feature of paramount importance in the inherently vulnerable Internet-based cloud computing landscapes. Comprehensive security and performance analyses confirm that Anony Control is both secure and efficient for cloud storage applications. Anony Control-F inherits the robust security framework of Anony Control, maintaining equivalent security levels, although it introduces additional communication overhead due to the 1-out-of-n oblivious transfer mechanism. One of the most promising directions for future work is the development of an efficient user revocation mechanism within our anonymous attribute-based encryption (ABE) frameworks. Supporting user revocation is crucial for real-world applications, where the ability to dynamically modify user access rights is essential. This introduces significant challenges in the application of ABE schemes, particularly in maintaining the balance between anonymity and dynamic access control. Further research will focus on making our schemes compatible with existing ABE systems that have already demonstrated efficient user revocation capabilities. This compatibility would significantly enhance the practical applicability and security of our approaches in diverse cloud computing scenarios.

REFERENCES

1. Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. In Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005), pp. 457-473.

2. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), pp. 321-334.

3. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89-98.

4. Liu, Z., Cao, Z., & Liang, K. (2010). Efficient Fully Secure Attribute-Based Encryption with Outsourcing Key-Issuing. In Proceedings of the 9th International Conference on Cryptology and Network Security (CANS 2010), pp. 78-91.

5. Wang, Q., Ren, K., Lou, W., & Li, Y. (2010). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE Transactions on Parallel and Distributed Systems, 22(5), 847-859.

6. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward Secure and Dependable Storage Services in Cloud Computing. IEEE Transactions on Services Computing, 5(2), 220-232.

7. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. In Proceedings of the 2010 IEEE INFOCOM, pp. 534-542.

8. Li, J., Li, Q., Jia, C., & Lee, J. (2014). Achieving Privacy in Cloud Storage with Access Control Based on Hierarchical Attribute-Based Encryption. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), pp. 3152-3157.

9. Zhang, R., & Liu, L. (2010). Security Models and Requirements for Healthcare Application Clouds. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), pp. 268-275.

10. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In Proceedings of the 29th Annual International Conference on the Theory and Applications of

Cryptographic Techniques (EUROCRYPT 2010), pp. 62-91.

11. Han, J., Susilo, W., & Mu, Y. (2012). Identity-Based Data Storage in Cloud Computing. Future Generation Computer Systems, 29(3), 673-681.

12. Zheng, Q., Xu, S., &Ateniese, G. (2012). VABKS: Verifiable Attribute-Based Keyword Search over Outsourced Encrypted Data. In Proceedings of the 2014 IEEE Conference on Computer Communications (INFOCOM), pp. 522-530.

13. Ruj, S., Nayak, A., &Stojmenovic, I. (2011). DACC: Distributed Access Control in Clouds. In Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 91-98.

14. Lai, J., Deng, R. H., Li, Y., & Weng, J. (2011). Fully Secure Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts and Fast Decryption. In Proceedings of the 2011 ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), pp. 293-302.

15. Zhang, L., Varadharajan, V., & Blanchard, J. (2014). Dynamic Attribute-Based Access Control for Multi-Authority Cloud Storage Systems. In Proceedings of the 2014 International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous), pp. 287-298.